AMENDMENTS TO THE CLAIMS

In the Claims:

The following listing of claims replaces all prior versions and listings of claims in the application.

Listing of Claims:

27. (Currently Amended) A method for protecting one or more computer systems using the same secret key (Ks) cryptographic algorithm, each computer system having storage means for storing the secret key (Ks) and processing means for executing the cryptographic algorithm, the method comprising:

~~characterized in that~~ storing a secret data (Ds) ~~stored~~ in a secret area of the storage means; ~~the computer system or systems is utilized to perform a cryptographic calculation for each computer system and for each secret key~~

separating a standard cryptographic algorithm into a plurality of simultaneous calculation processes based on the secret data (Ds);

creating a plurality of partial intermediate variables corresponding to each intermediate variable of the standard cryptographic algorithm;

applying nonlinear transformations to each of the plurality of partial intermediate variables to create a plurality of partial results; and

reconstituting a final result, corresponding to a result of the standard cryptographic algorithm, from the plurality of partial results.

28. (Currently Amended) The method according to claim 27, ~~characterized in that, for each computer system and for each secret key (Ks), the way in which said~~ wherein the secret data (Ds) ~~is used to perform said cryptographic calculation is public~~ includes:

a secret function f;

a plurality of partial conversion tables;

a secret random conversion table associated with a calculation based on conversion tables stored in a non-secret area of the storage means;

a polynomial function and one or more conversion tables;

a bijective secret function and a random secret transformation; and

a quadratic secret function.

29. (Currently Amended) The method according to claim 27, ~~characterized in that in~~ wherein, for each of the computer systems, ~~each~~ the secret key (Ks) ~~used by said cryptographic calculation corresponds to a specific piece of said~~ and the secret data (Ds) are entered into a programmable, non-volatile memory.

30. (Currently Amended) A method according to claim 27, ~~for protecting one or more computer systems~~ wherein the ~~cryptographic calculation uses~~ nonlinear transformations include nonlinear transformations of km bits into kn bits described by k conversion tables in which n output bits of the transformation are read at an address that is a function of the km input bits, and for each of said nonlinear transformations, said k tables are part of the secret data (Ds).

31. (Currently Amended) A method according to claim 27, ~~for protecting one or more computer systems~~ wherein the ~~cryptographic calculation process uses~~ nonlinear transformations include nonlinear transformations of km bits into kn bits described by k conversion tables in which n output bits of the transformation are read at an address obtained by applying a secret bijective function (φ) to an m-bit value, itself obtained by applying a public function of the km input bits of the nonlinear transformation, and for each of said nonlinear transformations, said k tables are part of the secret data (Ds).

32. (Currently Amended) The method according to claim 27, further comprising storing a conversion table calculation program in each computer system and activating the calculation program by a given event in order to calculate tables and store all or part of said tables in the secret data (Ds).

33. (Currently Amended) A computer system, comprising:

storage means for storing ~~a modified cryptographic algorithm that adheres to computational phases of a standard cryptographic algorithm,~~ a secret encryption key and ~~contained~~ secret data in a secret area of the storage means ~~for modifying the standard cryptographic algorithm,~~; and

at least one processor, coupled to the storage means, for modifying a standard secret key cryptographic algorithm into calculation processes based on the secret data, the processor operating to:

separate the standard secret key cryptographic algorithm into a plurality of simultaneous calculation processes based on the secret data,

~~means for executing said modified cryptographic algorithm,~~

~~first secret means for replacing~~ replace each intermediate variable[[s]] ~~required for the computational phases~~ of the standard secret key cryptographic algorithm with a plurality ~~(k)~~ of partial intermediate variables,

~~second means for applying a~~ apply nonlinear transformations ~~table~~ to each of ~~said~~ the plurality of partial intermediate variables to create a plurality of partial results, and

~~third secret means for reconstituting~~ reconstitute a final result, corresponding to ~~utilization~~ a result of the standard secret key cryptographic algorithm, from the plurality of partial results ~~obtained on the partial variables~~.

34. (Currently Amended) A computer system according to claim 33, ~~characterized in that~~ wherein the secret ~~encryption key~~ data stored in the secret area includes at least one first random variable v_1 constituting at least one secret partial variable, and the modified cryptographic algorithm determines at least one other partial variable v_2, by applying a first secret function to the intermediate variable v and the secret partial variable or variables v_1.

35. (Currently Amended) A computer system according to claim 34, ~~characterized in that~~ wherein:

the modified cryptographic algorithm includes tables used for applying the nonlinear transformations to the partial variables v_1 and v_2, at least one of said tables ~~(A)~~, formed by random selection, and being stored in the secret data ~~Ds~~, the other tables required for the calculations being stored in a nonvolatile memory, and

the processor executes ~~means for executing~~ various computational rounds of the standard algorithm, each time using the tables on the partial variables, and calculates ~~means for calculating~~ the final result in the last round of the algorithm by combining the partial ~~variables~~ results in accordance with a second secret function.

36. (Currently Amended) A computer system according to claim 33, ~~characterized in that the first secret means of the modified algorithm are constituted by~~ wherein the modified cryptographic algorithm includes a function *f*, linking the partial intermediate variables and each intermediate variable (v), such that the knowledge of one value of said

intermediate variable never makes it possible to deduce all of the particular partial values v_i such that there exists a *(k-1)-tuple* $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots v_k)$ that satisfies the equation $f(v_1, \ldots, v_i, \ldots, v_k) = v$.

37. (Currently Amended) A computer system according to claim 33, ~~characterized in that the second means of the modified algorithm are constituted by~~ wherein the secret data includes k partial conversion tables, and among the *k* partial conversion tables, *k-1* partial conversion tables contain secret random variables.

38. (Currently Amended) A computer system according to claim 36[[37]], ~~characterized in that the second means of the modified algorithm comprise~~ wherein the secret data includes k conversion tables, each of said conversion tables receiving an input a value obtained by applying a secret bijective function φ_1 to said function $f(v_1,\ldots, v_k)$ of the partial intermediate variables in accordance with the relation $\varphi_j \circ f(v_1, \ldots,v_k)$, $j \in [1,k]$, this application $\varphi_j \circ f(v_1,\ldots, v_k)$ being performed by direct evaluation of a resulting value, this resulting value, applied to the input of the conversion table, making it possible to read *n* output bits of the transformation at an address that is a function of these *m* input bits.

39. (Currently Amended) A computer system according to claim 33, ~~characterized in that the second means of the modified algorithm comprise means~~ wherein the processor operates to:

replace ~~for replacing~~ each nonlinear transformation applied to an intermediate variable of the standard cryptographic calculation process, without a separation, with a partial nonlinear transformation of *km* bits into *kn* bits applied to all of the partial intermediate variables, ~~means for calculating~~

calculate *(k-)n* of said output bits of this transformation as a polynomial function of the *km* input bits, and ~~means for reading~~

read the remaining *n* bits of said output bits by reading a conversion table in which the *n* remaining bits are read at an address that is a function of the *km* input bits.

40. (Currently Amended) A computer system according to claim 33, ~~characterized in that it further includes means for~~ wherein the processor sequentially ~~executing~~ executes operations performed by the modified algorithm in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts.

41. (Currently Amended) A computer system according to claim 33, ~~characterized in that it includes means for executing~~ wherein the processor executes, in interleaved fashion, operations performed in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts.

42. (Currently Amended) A computer system according to claim 33, ~~characterized in that it includes means for~~ wherein the processor simultaneously ~~executing~~ executes operations performed in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts, in the event of multiprogramming.

43. (Currently Amended) A computer system according to claim 33, ~~characterized in that it includes means for simultaneously executing in~~ wherein the at least one processor includes different processors working in parallel, simultaneously executing the operations performed in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts.

44. (Currently Amended) A computer system according to claim 33, ~~characterized in that it~~ wherein the secret data includes a conversion table calculation program stored in each computer system and ~~means for activation~~ activated by a given event of the calculation of the tables and for the storage of all or part of these tables in the secret data.

45. (Previously Presented) A computer system according to claim 33, further including a counter having means for storing a value that is incremented with each cryptographic calculation so as to constitute a given event for the activation, by activating means, of the calculation of the tables when a given value is exceeded.

46. (New) A method according to claim 31, wherein for each of the nonlinear transformations, the secret bijective function (φ) is also part of the secret data.

47. (New) A system according to claim 33, wherein the secret data includes a plurality of nonlinear transformation tables, each transformation table designed to be applied by the processor to a partial intermediate variable.